ref 7

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－164064

(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08	
12/26		Ｇ０６Ｆ　13/00	３５５
Ｇ０６Ｆ　13/00	３５５	Ｈ０４Ｌ　11/00	３１０Ｄ
Ｈ０４Ｌ　12/28			

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平8－325050

(22)出願日　平成８年(1996)12月５日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　平田　俊明
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　宮崎　聡
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

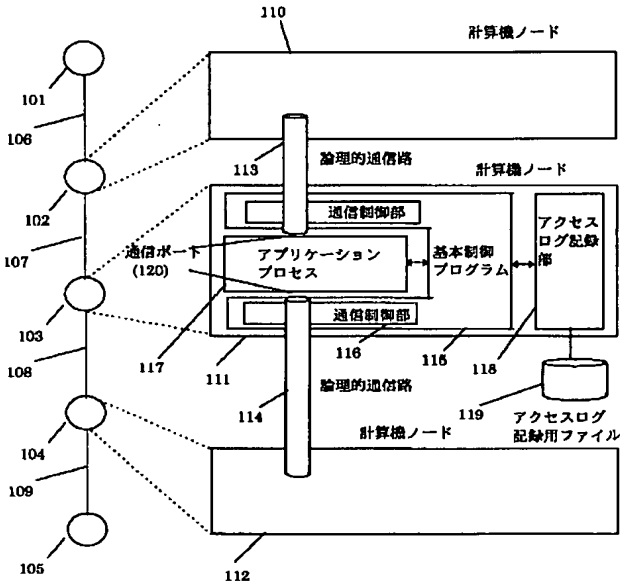
(54)【発明の名称】　ネットワーク侵入経路追跡方式

(57)【要約】

【課題】計算機を追跡するための必要十分な情報をアプリケーションプログラムに変更を加えることなく採取する。

【解決手段】第一ノード（以下Ｎ）で、第二Ｎからの論理的通信路が確立し、第一Ｎは第二Ｎに対してプロセスの識別子とユーザプロセスが第三Ｎから論理的通信路を介して起動された場合、通信ポートと第三Ｎの識別子を要求し、この情報と第一Ｎ上で第二Ｎからの論理的通信路に対応する通信ポートと対応するプロセスの識別子とともに記録する手段と、第一Ｎでセキュリティ上の問題検出の場合、第一Ｎ上の記録情報を参照し、第二Ｎからの接続であると認識し、第一Ｎ上の記録情報と第二Ｎ上で記録した同種の情報のうち第二Ｎに関するプロセスの識別子と通信ポートの識別子と通信相手Ｎの識別子を突き合わせて、一致したものを対応する記録情報とし前述と同種の記録情報を参照する。

図１



1

【特許請求の範囲】

【請求項１】通信ノード間を双方のノード上の通信ポートのペアで接続する論理的通信路で構成するネットワークシステムにおいて、第一のノードで、第二のノードからの論理的通信路が確立したときに、前記第一のノードは前記第二のノードに対して前記通信路を確立したプロセスの識別子とユーザプロセスが第三のノードから論理的通信路を介して起動されたものである場合、前記通信ポートの識別子と前記第三のノードの識別子を要求し、これらの情報と前記第一のノード上で前記第二のノードからの前記論理的通信路に対応する前記通信ポートの識別子と対応するプロセスの識別子とともに記録し、前記第一のノードでセキュリティ上の問題を検出した場合、前記第一のノード上の前記記録情報を参照することで、前記第二のノードからの接続であることを認識し、前記第一のノード上の前記記録情報と前記第二のノード上で記録した同種の情報のうち前記第二のノードに関するプロセスの識別子と前記通信ポートの識別子および通信相手ノードの識別子を突き合わせて、一致したものを対応する記録情報とみなして前記第三のノードの前記と同種の記録情報を参照にいくという手順を繰り返し侵入経路を特定することを特徴とするネットワーク侵入経路追跡方式。

【請求項２】請求項１において、前記第一のノードで、前記第二のノードからの論理的通信路が確立したときに、前記第一のノードは前記第二のノードに対して情報に加えて前記第二のノードが前記第三のノードからの論理的通信路が確立したときに、前記第三のノードから受け取った情報も要求するという手順を繰り返し、前記第一のノードでセキュリティ上の問題を検出した場合、前記第一のノード上の記録情報のみを参照することで侵入経路を特定するネットワーク侵入経路追跡方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワーク侵入経路追跡方式に関する。

【０００２】

【従来の技術】従来の計算機システムでは、例えば、ヒューレットパッカード社のオペレーティングシステムＨＰ－ＵＸやＴＣＰwrapperのようなソフトウエアを用いていつ、どこの計算機から接続されたという情報をログとして記録する方法がある。

【０００３】

【発明が解決しようとする課題】しかし、従来技術では、複数の計算機に順次接続しながら遠隔地の計算機を利用する場合、これらの計算機を追跡するための情報として十分でない。また、計算機上のアプリケーションが他の計算機に接続する時点で、接続先計算機や通信ポートに関する情報をログとして記録する方法も考えられるが、アプリケーションごとに本機能を追加する必要があり、アプリケーション開発の負荷となる。

2

【０００４】本発明の目的は、複数の計算機に順次接続しながら遠隔地の計算機を利用する場合、これらの計算機を追跡するための必要十分な情報をアプリケーションプログラムに変更を加えることなく採取し、これらの情報から順次接続した計算機を追跡し、発信元を特定する手段を提供することにある。

【０００５】

【課題を解決するための手段】上記の課題を解決するため、本発明では、第一のノードで、第二のノードからの論理的通信路が確立したときに、第一のノードは第二のノードに対して前記通信路を確立したプロセスの識別子と前記ユーザプロセスが第三のノードから論理的通信路を介して起動されたものである場合、前記通信ポートの識別子と第三のノードの識別子を要求し、これらの情報と第一のノード上で第二のノードからの論理的通信路に対応する通信ポートの識別子と対応するプロセスの識別子とともに記録する手段と、第一のノードでセキュリティ上の問題を検出した場合、第一のノード上の前記記録情報を参照することで、第二のノードからの接続であることを認識し、第一のノード上の前記記録情報と第二のノード上で記録した同種の情報のうち第二のノードに関するプロセスの識別子と通信ポートの識別子および通信相手ノードの識別子を突き合わせて、一致したものを対応する記録情報とみなして第三のノードの前記と同種の記録情報を参照する手段を有する。

【０００６】また、第一のノードで、第二のノードからの論理的通信路が確立したときに、第一のノードは第二のノードに対して前述の情報に加えて第二のノードが第三のノードからの論理的通信路が確立したときに、第三のノードから受け取った前述の情報も要求するという手順を繰り返す手段を有する。

【０００７】

【発明の実施の形態】図１に従って本発明の一実施例であるネットワーク侵入経路追跡方式を説明する。図１では計算機ノード１０１から１０２，１０３，１０４の各計算機ノードに順次接続しながら計算機ノード１０５を利用している様子を示している。各計算機ノード間は論理的通信路１０６～１０９で接続している。計算機ノード１１１の本発明に関する構成は、アプリケーションプロセス１１７が通信制御部１１６を介して接続すべき計算機ノード１１０に対して論理的通信路１１３を確立することで前記遠隔地の計算機ノード１１０上のアプリケーションプロセスを起動しこれを利用する。アプリケーションプロセスが論理的通信路を利用するためのアクセスポートが通信ポート１２０である。また、遠隔地の計算機ノード１１０は計算機ノード１１１と同様の構成である。アクセスログ記録部１１８は他の計算機ノードからの論理的通信路が確立したときに侵入経路の追跡に必要な情報をファイル１１９に記録する。基本制御プログ

ラム１１５はプロセスの実行制御やメモリの制御、ディスク装置との入出力制御に加えて通信制御処理も実行する。さらに、実行中のプロセスや通信ポートに関する情報を提供する。アプリケーションプロセスの例としてはＵＮＩＸシステムで利用されるtelnetやrloginなどがあり、ＴＣＰ／ＩＰネットワークでＩＰパケットが直接届かないネットワークに対しては特定の計算機ノードに一旦telnetまたはrloginで接続してから目的の計算機ノードにtelnetまたはrloginで接続するという手順を踏む必要がある。

【０００８】図２は各計算機ノードを構成するハードウエア構成を表す。計算機ノード２００は、各種演算等の命令を実行する中央処理装置２０２，演算に必要なデータを格納する主記憶装置２０１，通信回線やローカルエリアネットワークとのデータの入出力を制御するネットワーク制御装置２０３および通信回線２０５、ローカルエリアネットワーク２０４、ディスク装置２０７との入出力を制御するディスク制御装置２０８から構成する。

【０００９】図３および図４は本発明の一実施例である各計算機ノード上でのアクセスログの記録手順を示す。第一の計算機ノード［例えば図１で計算機ノード１１１］で第二の計算機ノードから論理的通信路が確立した場合、第一の計算機ノードは第二の計算機ノード［例えば図１で計算機ノード１１２］に対して経路追跡に必要な情報を要求する３０１。第二の計算機ノードは要求に対して、第二の計算機ノード上で第一の計算機ノードに対して接続要求を行なったアプリケーションプロセスが第三のノードから論理的通信路を介して起動されたものである場合４０１、通信路を確立したアプリケーションプロセスの識別子＋通信ポートの識別子と第三の計算機ノードの識別子を第一の計算機ノードへ返送する４０２。そうでない場合は４０１、通信路を確立したアプリケーションプロセスの識別子を第一の計算機ノードへ返送する４０３。第二の計算機ノードから追跡情報を受信した第一のノードは第二の計算機ノードから得た経路追跡に必要な情報＋第二の計算機ノードからの論理的通信路に対応する通信ポートの識別子と対応するプロセスの識別子をアクセスログ記録用ファイルに記録する３０２。経路追跡に必要な情報は第一の計算機ノードおよび第二の計算機ノードともに図１におけるアクセスログ記録部が基本制御プログラム介して取得する。このため、本実施例では基本制御プログラムが経路追跡に必要な情報を提供するためのインタフェースを有することが前提となるが、本発明の方式を用いることでアプリケーションプロセスはアクセスログ記録に関する制御を全く意識する必要がない。

【００１０】次に、第一のノードでセキュリティ上の問題を検出した場合の侵入経路の特定手段を図５を用いて説明する。図５では、第一の計算機ノードを５０４、第二の計算機ノードを５０３、第三の計算機ノードを５０２としている。ネットワーク管理マネージャ５０１は関連ノードから必要な情報を集めて侵入経路を特定する手段を持つ。例えば、計算機ノード５０４でセキュリティ上の問題が発生し、ネットワーク管理マネージャに非同期に通知したとする［５０５］。ネットワーク管理マネージャは通知を契機に計算機ノード５０４から問題の発生したアプリケーションプロセスに関するアクセスログ記録用ファイルに記録されたログ情報を参照する［５０６］。このログ情報から計算機ノード５０３からの接続であることを認識し、計算機ノード５０４上の記録情報と計算機ノード５０３上で記録した同種の情報のうち計算機ノード５０３に関するプロセスの識別子と通信ポートの識別子および通信相手ノードの識別子を突き合わせて、一致したものを対応する記録情報とみなして計算機ノード５０２の前述と同種の記録情報を参照にいくという手順を繰り返し［５０６］、侵入経路を特定するとともにローカルに起動されたアプリケーションプロセスの存在する計算機ノードに行き当たったとき、これを発信元と特定する。

【００１１】次に本発明の別の実施例であるネットワーク侵入経路追跡方式を図６および図７を用いて説明する。第一の計算機ノード（例えば図１で計算機ノード１１１）で第二の計算機ノードから論理的通信路が確立した場合、第一の計算機ノードは第二の計算機ノード（例えば図１で計算機ノード１１２）に対して経路追跡に必要な情報を要求する［６０１］。第二の計算機ノードは要求に対して、第二の計算機ノード上で第一の計算機ノードに対して接続要求を行なったアプリケーションプロセスが第三のノードから論理的通信路を介して起動されたものである場合［７０１］、通信路を確立したアプリケーションプロセスの識別子＋通信ポートの識別子と第三の計算機ノードの識別子＋第三の計算機ノードから既に受信済みのアクセスログへの記録情報、を第一の計算機ノードへ返送する［７０２］。そうでない場合は［７０１］、通信路を確立したアプリケーションプロセスの識別子を第一の計算機ノードへ返送する［７０３］。第二の計算機ノードから追跡情報を受信した第一のノードは第二の計算機ノードから得た経路追跡に必要な情報＋第二の計算機ノードからの論理的通信路に対応する通信ポートの識別子と対応するプロセスの識別子をアクセスログ記録用ファイルに記録する［６０２］。

【００１２】次に、図５における計算機ノード５０４でセキュリティ上の問題を検出した場合、ネットワーク管理マネージャは計算機ノード５０４から問題の発生したアプリケーションプロセスに関するアクセスログ記録用ファイルに記録されたログ情報を参照する。このログ情報は発信元からの接続経路情報が全て含まれているため、このログ情報のみから、第一の実施例で示した解析手順を用いることで侵入経路および発信元を特定することができる。

5

【００１３】

【発明の効果】本発明によれば、複数の計算機に順次接続しながら遠隔地の計算機を利用する場合、これらの計算機を追跡するための必要十分な情報をアプリケーションプログラムに変更を加えることなく採取し、これらの情報から順次接続した計算機を追跡し、発信元を特定する手段を提供することができる。さらに、請求項２の手段を用いれば、請求項１の手段に比べて順次接続する時点でのログ情報の転送トラヒックが増加するものの、侵入追跡は問題を検出したノードからのみログ情報を収集すればよく、侵入追跡時に関連する中継ノードが障害等でログ情報の収集ができない場合でも追跡が可能である。

【図面の簡単な説明】

【図１】各計算機ノードに順次接続しながら遠隔地の計算機ノードを利用している様子および各計算機ノードの構成を表す説明図。

【図２】計算機ノードのハードウエア構成例を表すブロック図。

【図３】第二の計算機ノードから論理的通信路の確立要求時の第一の計算機ノードにおけるアクセスログの取得手順を表すフローチャート。

6

【図４】第二の計算機ノードで第一の計算機ノードから経路追跡に必要な情報を要求された時点でのアクセスログの取得手順を表すフローチャート。

【図５】アクセスログを収集し侵入追跡を行なう場合の構成および手順を表す説明図。

【図６】第二の計算機ノードから論理的通信路の確立要求時の第一の計算機ノードにおけるアクセスログの取得手順を表すフローチャート。

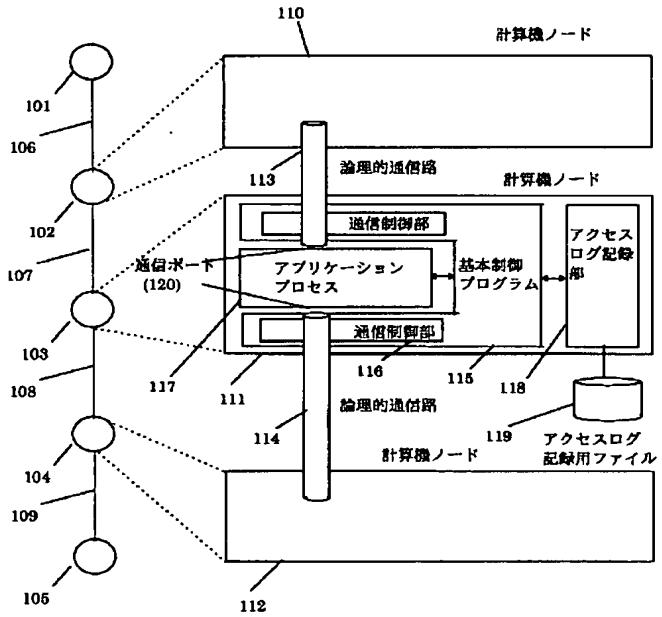
【図７】第二の計算機ノードで第一の計算機ノードから経路追跡に必要な情報を要求された時点でのアクセスログの取得手順を表すフローチャート。

【符号の説明】

１０１～１０５…計算機ノード、
１０６～１０９…論理的通信路、
１１５…基本制御プログラム、
１１６…通信制御部、
１１７…アプリケーションプロセス、
１１８…アクセスログ記録部、
１１９…アクセスログ記録用ファイル。

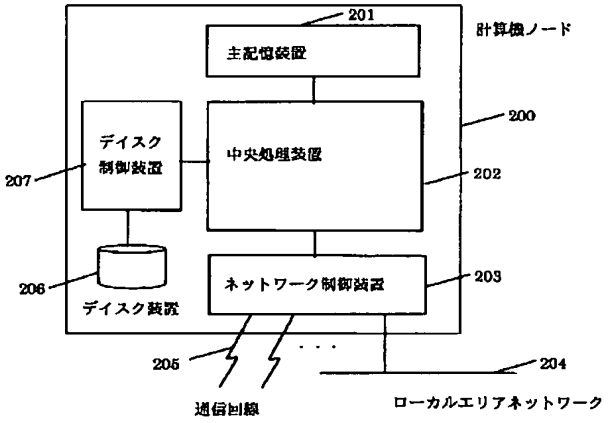
【図１】

図1



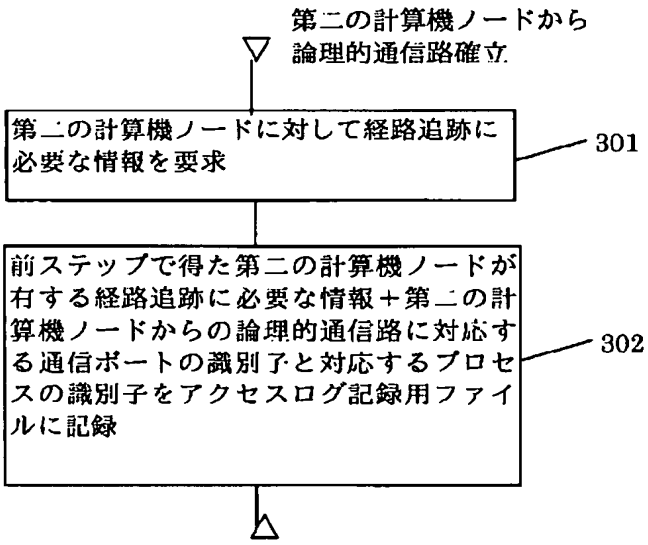
【図２】

図2



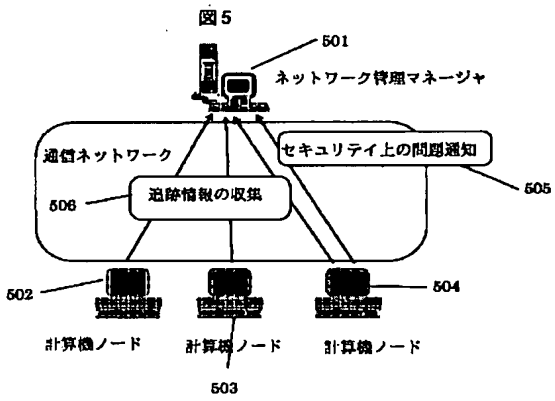
【図３】

図３



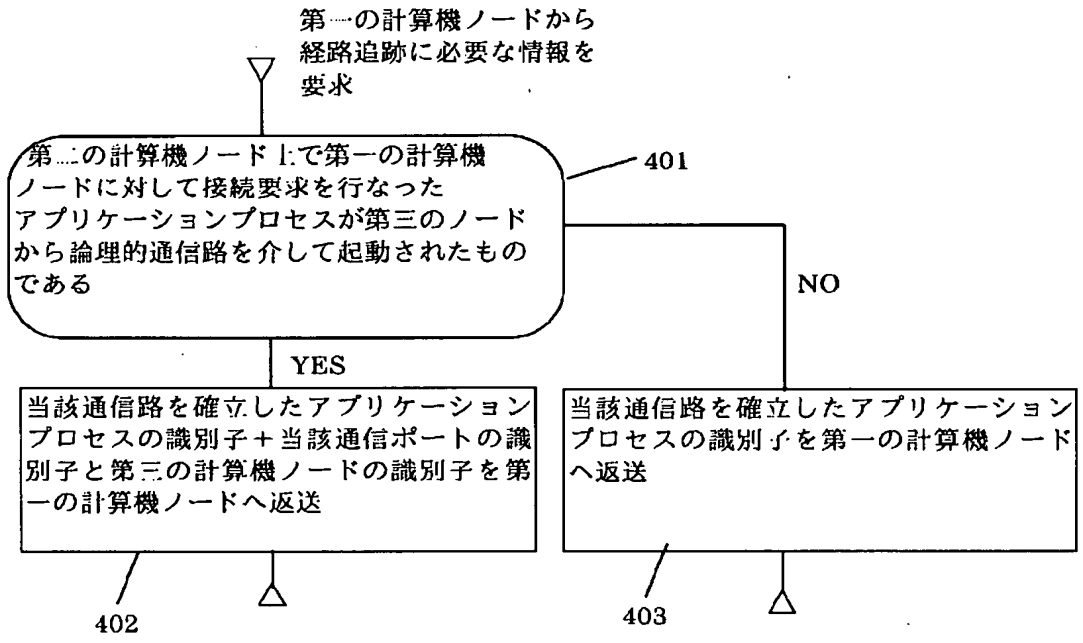
【図５】

図５



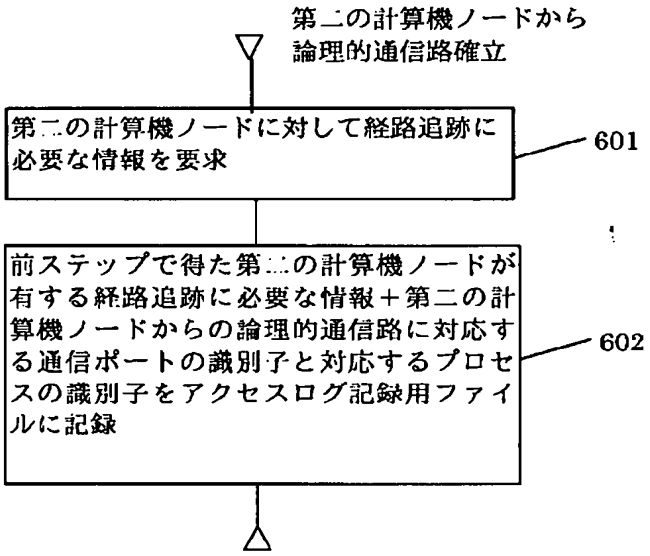
【図４】

図４



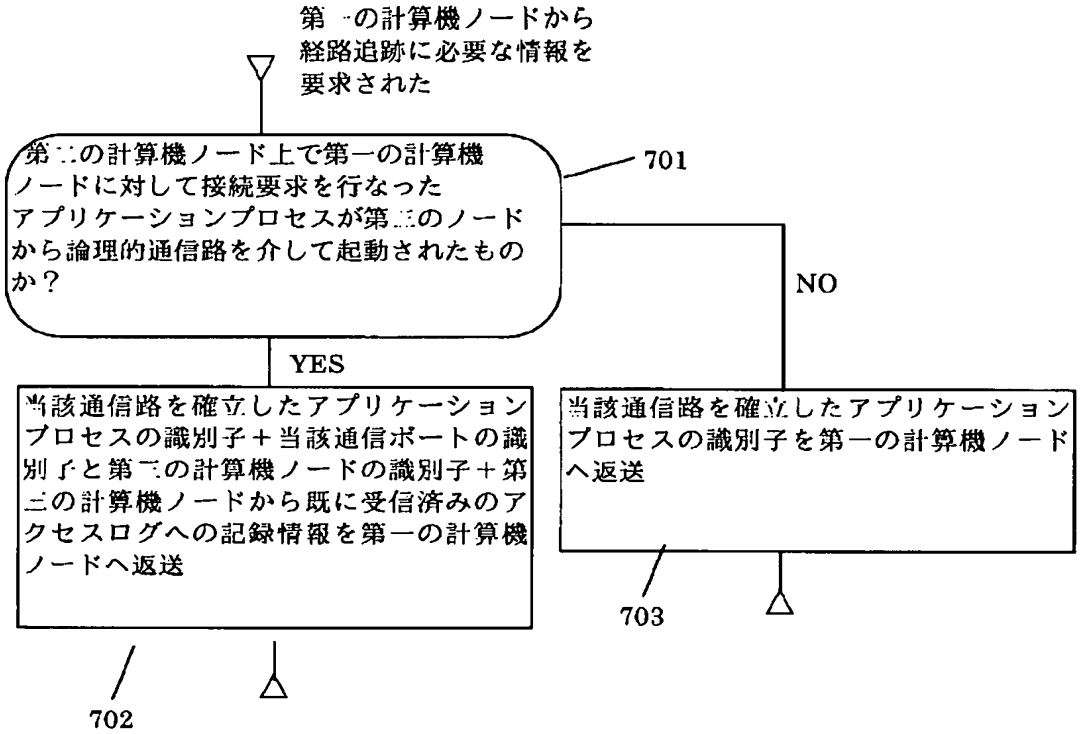
【図６】

図６


第二の計算機ノードから
論理的通信路確立
第二の計算機ノードに対して経路追跡に必要な情報を要求
601
前ステップで得た第二の計算機ノードが有する経路追跡に必要な情報＋第二の計算機ノードからの論理的通信路に対応する通信ポートの識別子と対応するプロセスの識別子をアクセスログ記録用ファイルに記録
602

【図７】

図７


第一の計算機ノードから
経路追跡に必要な情報を
要求された
第二の計算機ノード上で第一の計算機ノードに対して接続要求を行なったアプリケーションプロセスが第二のノードから論理的通信路を介して起動されたものか？
701
NO
YES
当該通信路を確立したアプリケーションプロセスの識別子＋当該通信ポートの識別子と第二の計算機ノードの識別子＋第二の計算機ノードから既に受信済みのアクセスログへの記録情報を第一の計算機ノードへ返送
当該通信路を確立したアプリケーションプロセスの識別子を第一の計算機ノードへ返送
703
702